1/3,AB,LS/3 (Item 1 from file: 351)
DIALOG(R)File 351:Derwent WPI

014106706
WPI Acc No: 2001-590918/ 200167
XRPX Acc No: N01-440172
Access to electronic documents transmitted over network to computer having local server
Patent Assignee: WITTKOETTER E (WITT-I)
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
DE 20003845	U1	20010712	DE 2000U2003845	U	20000301	200167	B

Priority Applications (No Type Date): DE 2000U2003845 U 20000301
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
DE 20003845	U1		19	H04L-009/00	

Abstract (Basic): DE 20003845 U1
Abstract (Basic):
NOVELTY - A local computer system (10) is connected with an external server (14)via a network (12), ie the internet. Data is exchanged via an interface (18) coupled to the controller (16). Electronic documents are stored temporarily in memory (22) and are decoded and transmitted as output by a local server module (24).
USE - Computer network systems
ADVANTAGE - Limits unauthorised access
DESCRIPTION OF DRAWING(S) - Block diagram
Computer (10)
Network server (14)
Network (12)
Memory (22)
Local server (24)
pp; 19 DwgNo 1/1

(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENT- UND MARKENAMT

(12) **Gebrauchsmusterschrift**

(10) **DE 200 03 845 U 1**

(51) Int. Cl.[7]:
H 04 L 9/00
G 06 F 12/14
// H04L 12/22

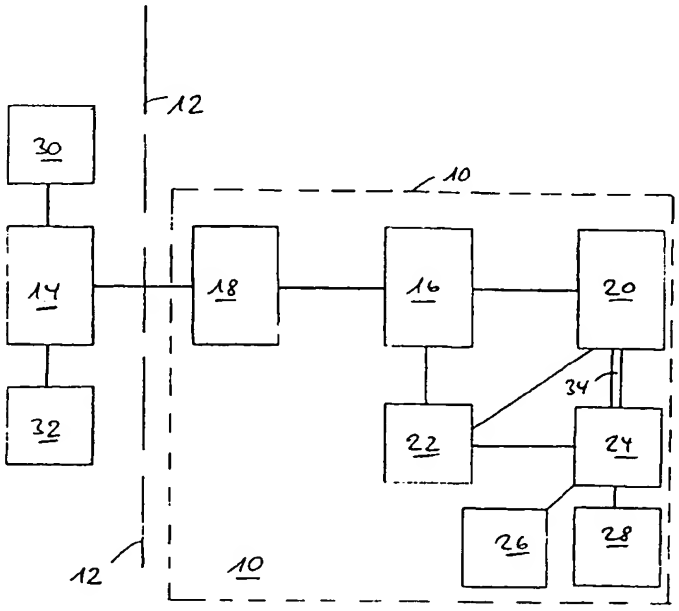
(21) Aktenzeichen: 200 03 845.1
(22) Anmeldetag: 1. 3. 2000
(47) Eintragungstag: 12. 7. 2001
(43) Bekanntmachung im Patentblatt: 16. 8. 2001

(73) Inhaber:
Wittkötter, Erland, Dr., Ermatingen, CH

(74) Vertreter:
Hiebsch Peege Behrmann, 78224 Singen

(54) Vorrichtung zum Zugreifen auf ein elektronisches Dokument

(57) Vorrichtung zum Zugreifen auf ein elektronisches Dokument als Reaktion auf einen Steuerbefehl, mit einer einer lokalen, elektronischen Datenverarbeitungsvorrichtung zugeordneten zentralen Steuer und Verarbeitungs einheit (16), einer durch die Steuer- und Verarbeitungseinheit ansprechbaren Datenkommunikationsschnittstelle (18), die einen Zugriff der elektronischen Datenverarbeitungsvorrichtung auf eine externe Servereinheit (14) über ein bevorzugt öffentlich zugängliches elektronisches Datennetz (12), insbesondere das Internet, ermöglicht, sowie einer durch die zentrale Steuer- und Verarbeitungseinheit angesprochenen, lokalen Speichereinheit (22) der Datenverarbeitungseinrichtung, die zum temporären und/oder dauerhaften Speichern elektronischer Dokumente ausgebildet ist, wobei die Datenverarbeitungseinrichtung (10) eine ohne Zwischenschaltung des elektronischen Datennetzes (12) durch eine lokale Darstellungseinheit der Datenverarbeitungsvorrichtung mittels elektronischer Datensignale nach dem TCP/IP-Protokoll ansprech- und zugreifbare lokale Servereinheit (24) aufweist,
die Datenverarbeitungseinrichtung so ausgebildet ist, dass elektronische Daten des elektronischen Dokuments in der lokalen Speichereinheit (22) in verschlüsselter Form speicherbar sind
und ein Entschlüsseln der verschlüsselten Daten und/oder ein Zugriff auf zugeordnete Schlüssel- oder Rekonstruktionsdaten sowie ein Darstellen des elektronischen Dokuments in unverschlüsselter Form durch Zugriff der Darstellungseinheit auf die lokale Servereinheit erfolgt.



DE 200 03 845 U 1

HIEBSCH PEEGE BEHRMANN
PATENTANWÄLTE
EUROPEAN PATENT AND TRADEMARK ATTORNEYS

Antrag auf Eintragung eines Gebrauchsmusters

Unser Zeichen: *W223DE7*
B/mü

(31) ***Prioritätsnummer / Priority Application Number:***

(32) ***Prioritätstag / Priority Date:***

(33) ***Prioritätsland / Priority Country:***

(54) ***Titel / Title:***

Vorrichtung zum Zugreifen auf ein elektronisches Dokument

(71) ***Anmelder/in / Applicant:***

Dr. Erland Wittkötter
Schönhaldestr. 21

8272 Ermatingen
Schweiz

(74) ***Vertreter / Agent:***

Dipl.-Ing. Gerhard F. Hiebsch
Dipl.-Ing. Dr. oec. Niels Behrmann M.B.A. (NY)
Heinrich-Weber-Platz 1

78224 Singen

Vorrichtung zum Zugreifen auf ein elektronisches Dokument

Die vorliegende Erfindung betrifft eine Vorrichtung zum Zugreifen auf ein elektronisches Dokument, etwa in Form eines PC, wobei dieser PC eine zentrale Steuer- und Verarbeitungseinheit aufweist, mit welcher eine interne PC-Datenkommunikations-Schnittstelle angesprochen werden kann, womit wiederum, etwa mittels geeigneter Zugriffs-Software, auf externe Server über geeignete (z.B. öffentlich zugängliche) Datenübertragungsnetze, etwa das Internet, zugegriffen werden kann.

Üblicherweise weist der PC zusätzlich eine lokale Speichereinheit auf, die, beispielsweise als Arbeitsspeicher oder als Festplattenspeicher realisiert, zum flüchtigen oder dauerhaften Speichern von Betriebs- und Dokumentdaten ausgebildet ist.

Eine derartige und bekannte Vorrichtung ermöglicht insbesondere auch den Zugriff auf elektronische Dokumente über das elektronische Datennetz, wie sie von einem geeigneten externen Server zur Verfügung gestellt werden können; der Begriff "elektronisches Dokument" im Rahmen der vorliegenden Erfindung soll dabei weit gefasst werden, und insbesondere Dateiprodukte gängiger Nutzeranwendungen sollen als elektronische Dateien im Sinne der vorliegenden Erfindung verstanden werden, einschließlich Bild-, Grafik-, Kalkulations-, Video-, Audio-, Datenbank-, Projektplanungs-, interaktive Annimations-, Spiele- oder Programmcode-Dateien.

Vor dem Hintergrund des Urheberrechtsschutzes kommerziell wertvoller Dateien und/oder einer Zugriffsbeschränkung auf vertrauliche elektronische Dateien stellt allgemein die Datenübertragung über das Internet bzw. der Zugriff auf elektronische Dateien eines externen Server ein Problem dar, da

veröffentlichter Inhalt praktisch unkontrolliert geladen und weiterverbreitet werden kann; insbesondere eine Sicherung der berechtigten Interessen eines Schöpfers an einem urheberrechtlich wertvollen und schutzfähigen Wert kann so nicht erfolgen.

Aus dem Stand der Technik ist es zwar bekannt, vertraulichen bzw. wertvollen Inhalt nur nach dem Durchführen eines entsprechenden Bezahlungsdialoges, z.B. nach Eingabe einer entsprechenden Kreditkarten-Nummer, und weiteren Zahlungsdaten, zum Herunterladen von dem externen Server freizugeben. Auch diese Lösung ist jedoch nur begrenzt praktikabel, da nach einem einmaligen, legalen Beschaffen dann wiederum die so erhaltene elektronische Datei mit dem elektronischen Dokument unbegrenzt weiterverteilt werden kann.

Als weitere Lösung aus dem Stand der Technik ist es bekannt, auf dem externen Server elektronische Dateien in verschlüsselter Form zugänglich zu machen (oder diese auf andere Weise, z.B. als Volumendaten verschlüsselt über CD-Roms zu verteilen), wobei dann eine sinnvolle Nutzung des zu schützenden Inhaltes nur nach (dauerhaftem oder zumindest einmaligem) Internet-Zugang zu einem entsprechenden Autorisierungs- bzw. Entschlüsselungsserver erfolgen kann. Bei entsprechender Gestaltung eines solchen autorisierten Zugriffsvorganges kann damit zwar eine effiziente Zugriffskontrolle erfolgen, allerdings ist, gerade zur Verwendung mit mobilen oder portablen Computersystemen, das Erfordernis eines externen Serverzuganges, insbesondere bei einem erneuten Zugreifen auf ein elektronisches Dokument, wenig praktikabel.

Aufgabe der vorliegenden Erfindung ist es daher, die Nachteile bekannter Zugriffsschutz- und Urheberrechts-Sicherungssysteme, die über elektronische Datennetze verteilbare elektronische Dokumente zum Gegenstand haben, da-

hingehend zu verbessern, dass insbesondere auch ohne regelmäßigen Internet-Kontakt (also etwa zu Beginn jeder Session, oder während der Dauer derselben) ein Zugriff auf ein wirksam gegen unautorisiertes Kopieren und Weitergeben geschütztes elektronisches Dokument möglich ist.

Die Aufgabe wird durch die Vorrichtung mit den Merkmalen des Anspruches 1 gelöst; vorteilhafte Weiterbildungen der Erfindung sind in den Unteransprüchen beschrieben.

So simuliert die erfindungsgemäß vorgesehene lokale Servereinheit die Funktion eines externen (d.h. über das elektronische Datennetz zugreifbaren) Hosts, in dem insbesondere auch der Zugriff mittels Datenpaketen nach TCP/IP erfolgt.

Von ansonsten bekannten TCP/IP-Anwendungen in einem lokalen Computersystem unterscheidet sich die vorliegende Erfindung dadurch, dass die Rolle der lokalen Servereinheit darin besteht, einen Entschlüsselungsvorgang der in verschlüsselter Form lokal gespeicherten Daten zu ermöglichen. Dies kann im Rahmen der Erfindung auf zwei Weisen geschehen: Zum einen kann die lokale Servereinheit die zum Entschlüsseln des lokal und verschlüsselt gespeicherten elektronischen Dokuments notwendigen Schlüssel- bzw. Rekonstruktionsdaten zum Zugriff durch die Darstellungseinheit anbieten, wobei dann durch eine geeignete Funktionalität der Darstellungseinheit die (bevorzugt temporäre) Rekonstruktion des elektronischen Dokuments in der für einen Benutzer brauchbaren Form erfolgt (insoweit also etwa ein geeignetes Plug-in in der Darstellungseinheit für die Wiederherstellung sorgt). Zum anderen kann die lokale Servereinheit selbst die Rekonstruktion des brauchbaren elektronischen Dokuments vornehmen und in vorbestimmter Weise (insbesondere ebenfalls temporär und zugriffsgeschützt) der Darstellungseinheit zur Darstellung für den Benutzer anbieten.

Diese technische Realisierung bietet gegenüber dem Stand der Technik zahlreiche Vorteile: Nicht nur reicht es aus, etwa durch einmaligen externen Serverkontakt über das Internet die Schlüssel- bzw. Rekonstruktionsdaten autorisiert zu beschaffen (ggf. zusammen mit den Daten des elektronischen Dokuments in der verschlüsselten Form); die lokale Servereinheit bietet dann im Rahmen der Erfindung (nach wie vor) dasjenige Sicherungs- bzw. Zugriffsumfeld, um nachfolgende, rein lokale Zugriffe auf das elektronische Dokument kontrolliert zu gestalten und insoweit für den (weiteren) Copyright-Schutz zu sorgen. So gehört es zu einer besonders bevorzugten Ausführungsform, die Datenverarbeitungsvorrichtung, insbesondere die Darstellungseinheit sowie die lokale Servereinheit, so auszugestalten, dass zu keinem Zeitpunkt das elektronische Dokument in der unverschlüsselten Form abspeicherbar und/oder nach extern (d.h. über eine Schnittstelle od.dgl.) ausles- oder übertragbar ist.

Gemäß einer bevorzugten Weiterbildung ist insbesondere auch vorgesehen, die (PC-interne) Datenkommunikationsleitung zwischen Darstellungseinheit und lokaler Servereinheit durch Verschlüsselung zu sichern, so dass nicht auch an dieser Stelle ein Angriff auf Daten des unverschlüsselten und damit wertvoll elektronischen Dokuments erfolgen kann.

In besonders bevorzugter Weise erfolgt ein Datenzugriff auf die lokale Servereinheit mittels einer (weitgehend frei wählbaren) Portadresse, die jedoch nicht einer standardmässig bestimmten Diensten zugewiesenen Portnummer entspricht (wie z.B. Port 80 für HTTP ist). Dabei ist es besonders bevorzugt, diese Portadresse oberhalb des Wertes 1024 zu wählen.

Ein Zugriff kann technisch mittels der TCP-IP-Adressierung 127.0.0.1 (localhost) erfolgen.

Für die Verschlüsselung der in der lokalen Speichereinheit abgelegten elektronischen Daten des elektronischen Dokuments (dies kann sowohl eine Adresse innerhalb der lokalen Servereinheit sein, als auch ein freigewählter elektronischer Speicherbereich außerhalb der lokalen Servereinheit) bietet es sich einerseits an, einen herkömmlichen, leistungsfähigen mathematischen Algorithmus zu verwenden. Ergänzend oder alternativ hat es sich jedoch als besonders bevorzugt herausgestellt, hier das Instrument der sog. semantischen Verschlüsselung zu verwenden, wie sie im Unteranspruch 7 erläutert ist und vom Anmelder zum Gegenstand früherer Schutzrechtsanmeldungen gemacht worden ist, etwa in den deutschen Patentanmeldungen 199 32 703.2, 199 62 902.1 sowie 199 53 055.6 als Verfahren zum Verschlüsseln einer elektronisch gespeicherten, ursprünglichen Datenmenge. Diese Technologie ist hinsichtlich der dort beschriebenen Erzeugung des Schlüssels bzw. der Entschlüsselung als vollumfänglich in die vorliegende Anmeldungsbeschreibung als zur Erfindung gehörig einbezogen.

Durch die vorliegende Erfindung wird somit ein komplexer, insbesondere auch Sicherungsaufgaben ermöglichender aktiver Prozess so zu einer lokalen Datenverarbeitungseinheit (Client) verlagert, dass einerseits dessen Benutzungs- und Bedienkomfort -- bei gleichbleibender Sicherheit -- beträchtlich erhöht werden kann, und andererseits die Möglichkeiten zum Umgang mit Daten auf Benutzerseite, gegenüber lediglich passiver Speicherung, wie aus dem Stande der Technik bekannt, beträchtlich erweitert sind.

Weitere Vorteile, Merkmale und Einzelheiten der Erfindung ergeben sich aus der nachfolgenden Beschreibung bevorzugter Ausführungsbeispiele sowie anhand der Zeichnungen; diese zeigen in:

Fig. 1: ein schematisches Blockschaltbild einer bevorzugten Ausführungsform der vorliegenden Erfindung (best mode).

Eine lokale Computereinheit 10 ist über ein öffentlich zugängliches Datennetz 12, insbesondere das Internet, mit einer externen Servereinheit 14 (Webserver) verbindbar. Genauer gesagt weist die lokale Computereinheit 10, die beispielsweise mittels eines herkömmlichen PC realisiert sein kann, eine ansonsten bekannte Steuereinheit 16 zum Koordinieren und Durchführen der Betriebsaktivitäten der lokalen Computereinheit 10 auf, so insbesondere auch das Zugreifen auf die externe Servereinheit 14 über das Internet 12 mittels einer der lokalen Computereinheit 10 zugeordneten Datenkommunikationsschnittstelle 18, die vorzugsweise mittels einer (in der Figur nicht gezeigten) Firewall in ansonsten bekannter Weise auf das Datenkommunikationsnetz 12 zugreifen kann.

Zentrale Funktionseinheit zur Bearbeitung und Darstellung der elektronischen Dateien im Rahmen der vorliegenden Erfindung ist eine Darstellungseinheit (Viewer) 20, die typischerweise in Form einer gängigen Internet-Browser-Software mit entsprechenden Funktionalitäten realisiert ist und (in ansonsten bekannter Weise) den externen Serverzugriff über das Internet 12 mittels eines Datenkommunikationsprotokolls nach dem TCP/IP-Standard sowie geeigneter Datenkommunikationsprotokolle, etwa HTTP, durchführen kann. Zu diesem Zweck ist die Datenkommunikationsschnittstelle 18 (bzw. eine ebenfalls zugeordnete Firewall) entsprechend und in übli-

cher Weise konfiguriert, etwa durch Freischalten der protokollgemäß üblichen Standardports bzw. Portadressen.

Sowohl die zentrale Steuereinheit 16, als auch die Darstellungseinheit 20 können in der lokalen Computereinheit 10 auf eine Datenspeichereinheit 22 zugreifen, die typischerweise als Festwert- bzw. Massenspeicher konfiguriert ist und im vorliegenden Ausführungsbeispiel zum Aufnehmen von verschlüsselten Volumendaten der elektronischen Dateien ausgebildet ist. Mit dem Begriff "Volumendaten" im Rahmen der vorliegenden Erfindung ist dabei ein Datenkörper der elektronischen Dateien gemeint, der bereits einen nicht unbeträchtlichen Teil der Gesamtdaten eines elektronischen Dokuments (oder mehrerer elektronischer Dokumenten) umfasst, wobei im vorliegenden Ausführungsbeispiel die Volumendaten jedoch verschlüsselt sind, d.h. nicht in einer für einen Benutzer vorgesehenen und brauchbaren Weise vorliegen. Neben den eingangs erläuterten Methoden der sog. semantischen Verschlüsselung kommt für das Verschlüsseln der Volumendaten in der Datenspeichereinheit 22 insbesondere auch das Anwenden gängiger mathematischer Verschlüsselungsalgorithmen in Betracht.

Um nunmehr ein gewünschtes elektronisches Dokument mittels der Darstellungseinheit (Viewer) 20 einem Benutzer zugänglich zu machen, ist im Ausführungsbeispiel der Fig. 1 eine lokale Servereinheit 24 vorgesehen, die -- innerhalb der lokalen Computereinheit 10 -- die Rolle und Betriebsweise der externen Servereinheit 14 simuliert und in entsprechender Weise mittels TCP/IP durch die Viewer-Einheit 20 angesprochen werden kann. Zu diesem Zweck ist der lokalen Servereinheit 24 sowohl eine lokale Nutzungsrecht- bzw. User-Verwaltungseinheit 26 zugeordnet, als auch eine Dokumentverwaltungseinheit 28. Die lokale Servereinheit 24 dient dabei u.a. zum gesicherten Speichern von Schlüssel- bzw. Rekonstruktionsdaten, wie sie über das Internet 12 und die

externe Servereinheit 14 von einer dieser zugeordneten Remote-Speichereinheit 30 beschafft werden können, und die Nutzungsrecht- und Userverwaltungseinheit 26 korrespondiert mit einer externen Servereinheit 14 zugeordneten Remote-Nutzungsrechtsvergabe-Einheit 32. So ermöglicht es die Nutzungsrecht- und Userverwaltungseinheit 26, einen am lokalen System 10 arbeitenden, zugreifenden Benutzer zu identifizieren und zum Zugriff auf die lokale Servereinheit 24, mithin die darin abgelegten Daten, zu authentifizieren.

Die Funktionsweise dieser Vorrichtung soll zur weiteren Verdeutlichung an einem Beispiel erläutert werden. Dabei wird angenommen, dass ein Benutzer der lokalen Computereinheit 10 Zugriff auf ein urheberrechtlich wertvolles elektronisches Textdokument nehmen möchte und auch bereit ist, dafür entsprechende Nutzungsrechte zu erwerben. Konkret richtet also der Nutzer mittels der Darstellungseinheit 20 der lokalen Computereinheit eine entsprechende Zugriffsanfrage in ansonsten bekannter Weise über das Internet 12 an die zur elektronischen Dokumentpublikation vorgesehene externe Servereinheit 14. Ohne dass der Benutzer sich vorerst hier konkret identifizieren muss oder einer Autorisierung bedarf, hat er die Möglichkeit, die verschlüsselten Volumendaten des elektronischen Dokuments aus der der externen Servereinheit 14 zugeordneten Speichereinheit 30 zu laden und -- verschlüsselt -- in der lokalen Datenspeichereinheit 22 seiner lokalen Computereinheit 10 abzulegen (alternativ hat er die Möglichkeit, sich diese verschlüsselten Volumendaten aus anderen Quellen zu beschaffen, etwa aus öffentlich zugänglichen weiteren Server-Sites, oder mittels ungeschützt verteilter Distributionsmedien, etwa CD-Roms).

Ein lokaler Zugriff auf ein entschlüsseltes und damit brauchbares elektronisches Dokument ist zu diesem Zeitpunkt dem Nutzer jedoch nicht möglich.

Vielmehr muss er, um das elektronische Dokument aus den geladenen Volumendaten entschlüsseln zu können, sich eine Rekonstruktions- bzw. Schlüsseldatei beschaffen, wobei dies im darstellten Ausführungsbeispiel wiederum durch Zugriff auf die externe Servereinheit 14 geschieht und aus der Remote-Speichereinheit 30 eine solche Rekonstruktions- bzw. Schlüsseldatei geladen werden kann. Dies ist jedoch nunmehr an das Erwerben eines entsprechenden Nutzungsrechts geknüpft, so dass ein Laden dieser Schlüsseldatei erst nach dem Durchführen einer entsprechenden Autorisierung bzw. einem von der Remote-Nutzungsrechtsvergabe-Einheit initiierten Bezahlungsdialogs (im Rahmen dessen der User z.B. Kreditkartendaten eingibt) möglich ist. Auch das Überlassen der Rekonstruktions- bzw. Schlüsseldaten mit dem Zweck des Ermöglichens eines legalen Benutzerzugriffes auf die elektronischen Daten hat jedoch nicht die Absicht, das elektronische Dokument danach frei und beliebig übertragbar zu gestalten; vielmehr soll auch der lokale Benutzerzugriff kontrollierbar und an festlegbare Zugriffsregeln geknüpft sein. Im vorliegenden Ausführungsbeispiel wird daher angenommen, dass mit der Zahlungstransaktion der Benutzer das Recht erwirkt, das elektronische Dokument beliebig häufig anzusehen, nicht jedoch das Dokument (unverschlüsselt) zu übertragen oder auszudrucken; ein typisches Ausführungsbeispiel für diese Form der elektronischen Dokumentpublikation wäre ein elektronisches Handbuch od.dgl. Eine solche Funktionalität im Rahmen der Erfindung kann insbesondere realisiert werden durch entweder eine entsprechende, durch die lokale Servereinheit 24 gesteuerte Einstellung des Viewers, oder aber mittels über die Verbindung 34 (zusammen mit weiteren Inhaltsdaten) übertragenen Steuerungs- bzw. Metadaten-, die - in der Art etwa einer Scriptsprache wie Javascript, Visual Basic Script, Java oder HTTP - die nicht mit Nutzungsrechten versehenen Aufgabenfunktionen des Viewers deaktiviert oder unterdrückt.

Im Rahmen des gezeigten Ausführungsbeispiels der vorliegenden Erfindung überträgt daher nach erfolgter Autorisierung die externe Servereinheit 14 die dem gewünschten elektronischen Dokument zugehörigen Entschlüsselungs- bzw. Rekonstruktionsdaten als Datei zur lokalen Computereinheit, wo diese Datei jedoch nicht in der lokalen Datenspeichereinheit 22 abgelegt wird, sondern in der lokalen Servereinheit 24 (diese Funktion läßt sich z.B. durch ein Plug-In der Viewer-Einheit 20 realisieren). Gleichzeitig werden die mit dem gewünschten elektronischen Dokument verbundene Zugriffs- bzw. Nutzungsrechte übertragen und in der lokalen Nutzungsrecht-Verwaltungseinheit 26 (unter Kontrolle der lokalen Servereinheit 24) abgelegt.

Der Nutzer hat nunmehr die Möglichkeit, mittels der lokalen Darstellungseinheit 20 das gewünschte elektronische Dokument im Rahmen der ihm zugewiesenen Nutzungsrechte zu aktivieren bzw. zu betrachten, und zwar wiederum durch entsprechende Funktionalität der lokalen Viewer- bzw. Darstellungseinheit (etwa realisiert wiederum mittels Plug-In): Die Darstellungseinheit 20 greift auf die Datenspeichereinheit 22 mit den verschlüsselten Volumendaten zu, und holt dann die Entschlüsselungs- bzw. Rekonstruktionsdaten aus der lokalen Servereinheit 24 (über eine besonders gegen unberechtigten Zugriff geschützte, verschlüsselte Verbindung 34 zwischen Viewer und lokaler Servereinheit). Der Viewer 20 rekonstruiert dann das elektronische Dokument in die unverschlüsselte, brauchbare Form und bietet es dem Nutzer in der durch das zugehörige Nutzungsrecht vorgesehenen Form an, etwa zur Betrachtung über einen Bildschirm. Eine besondere Funktionalität der Darstellungseinheit 20 (im Zusammenwirken mit der lokalen Servereinheit 24) besteht zudem darin, dass auch noch diese Vorgänge gegen unberechtigte Zugriffe auf das unverschlüsselte Dokument gesichert sind, etwa dadurch, dass, falls keine entsprechende Autorisierung vorliegt, ein Ausdrucken bzw. Abspeichern des unverschlüs-

selten Dokuments unmöglich ist. Die der lokalen Servereinheit 24 zugeordnete Dokumentverwaltungseinheit dient zusätzlich dazu, das elektronische Dokument in der Art einer Libray in einer für den Benutzer gewünschten Form zu organisieren, insbesondere ein Management von value-added Zusatzfunktionen durchzuführen, wie in der deutschen Patentanmeldung 199 62 902.1 des Anmelders offenbart ist und hinsichtlich der Schutzwirkung durch die Zusatzfunktionen in die vorliegende Erfindung einbezogen sein soll.

Die Ausführungsform gemäß Fig. 1 zeigt noch eine weitere, alternative Vorgehensweise zum Rekonstruieren des gewünschten elektronischen Dokuments: So ist es alternativ oder ergänzend möglich, durch Funktionalität der lokalen Servereinheit 24 die Rekonstruktion des unverschlüsselten, brauchbaren elektronischen Dokuments durchzuführen (durch unmittelbaren Zugriff auf die lokale Datenspeichereinheit 22 mit den verschlüsselten Volumendaten sowie durch Verknüpfen mit den in der lokalen Speichereinheit nach dem erfolgten externen Serverzugriff abgelegten Schlüssel- bzw. Rekonstruktionsdaten), wobei dann über die verschlüsselte bzw. gesicherte Leitung 34 -- typischerweise wird hierfür das SSLP (Secure-Socket-Layer-Protokoll) eingesetzt -- das entschlüsselte Dokument der Viewereinheit 20 zur Darstellung im Rahmen der vorgesehenen Nutzungsrechte angeboten wird.

Im gezeigten Ausführungsbeispiel kommuniziert die Viewer-Einheit 20 über die TCP/IP-Adresse 127.0.0.1 (localhost) mit der lokalen Servereinheit 24, wobei jedoch die lokale Servereinheit 24, wie gesagt, die Funktionalität des externen Webservers 14 mit geeigneten serverspezifischen Zugriffs- und Kontrollmöglichkeiten lokal implementiert. Damit ist dann die Möglichkeit gegeben, ohne fortgesetzten Remote-Zugriff (und damit etwa ohne Internet-Zugriffsmöglichkeit, wie auf einem transportablen Computer-

system) die vorteilhaften Zugriffs- und Verwaltungsrechte zum Schutz von urheberrechtlich wertvollem Dokumentinhalt beizubehalten, so dass im Ergebnis eine beträchtliche Flexibilisierung der bekannten, Internet-gestützten Prozesse erfolgen kann. Prinzipiell bewirkt also diese Verlagerung der bekannten Internet-Zugriffs- und Sicherungsprozesse in einen lokalen Prozess eine aktivere Funktion lokal abgespeicherter (traditionell lediglich passiver) Daten, wobei zusätzlich durch die Erfindung in vorteilhafter Weise die systembedingt beschränkten Zugriffsmöglichkeiten von lokalen Browser-Einheiten auf lokale Systemressourcen genutzt werden, um den für eine urheberrechtswahrende Distribution elektronischer Dokumente so wichtigen Zugriffssteuerungs- und Sicherungsaspekt zu realisieren.

Die vorliegende Erfindung ist nicht auf das gezeigte Ausführungsbeispiel beschränkt; so liegt es im Rahmen des einschlägigen Fachmannes, das in Fig. 1 beschriebene System je nach Anwendungsfall zu modifizieren, etwa durch ergänzende Funktionalitäten der lokalen Servereinheit (bzw. einer zugeordneten Dokumentverwaltungseinheit 28), die für weitere Web-Serverzugriffe 14, in Abhängigkeit von Benutzerwünschen, die nötigen Voraussetzungen schafft. Alternativ ist es von der vorliegenden Erfindung umfasst, auch die Volumendaten, die im Ausführungsbeispiel in der lokalen Datenspeichereinheit 22 gespeichert sind, der lokalen Servereinheit 24 zuzuordnen, wobei dann über die Nutzungsrechtsvergabe hier der prinzipiell auf die verschlüsselten Daten offene Zugriff geregelt werden kann.

ANSPRÜCHE

1. Vorrichtung zum Zugreifen auf ein elektronisches Dokument als Reaktion auf einen Steuerbefehl, mit
einer einer lokalen, elektronischen Datenverarbeitungsvorrichtung zugeordneten zentralen Steuer- und Verarbeitungseinheit (16), einer durch die Steuer- und Verarbeitungseinheit ansprechbaren Datenkommunikationsschnittstelle (18), die einen Zugriff der elektronischen Datenverarbeitungsvorrichtung auf eine externe Servereinheit (14) über ein bevorzugt öffentlich zugängliches elektronisches Datennetz (12), insbesondere das Internet, ermöglicht, sowie einer durch die zentrale Steuer- und Verarbeitungseinheit angesprochenen, lokalen Speichereinheit (22) der Datenverarbeitungseinrichtung, die zum temporären und/oder dauerhaften Speichern elektronischer Dokumente ausgebildet ist,
wobei die Datenverarbeitungseinrichtung (10) eine ohne Zwischenschaltung des elektronischen Datennetzes (12) durch eine lokale Darstellungseinheit der Datenverarbeitungsvorrichtung mittels elektronischer Datensignale nach dem TCP/IP-Protokoll ansprech- und zugreifbare lokale Servereinheit (24) aufweist,
die Datenverarbeitungseinrichtung so ausgebildet ist, dass elektronische Daten des elektronischen Dokuments in der lokalen Speichereinheit (22) in verschlüsselter Form speicherbar sind
und ein Entschlüsseln der verschlüsselten Daten und/oder ein Zugriff auf zugeordnete Schlüssel- oder Rekonstruktionsdaten sowie ein Darstellen des elektronischen Dokuments in unverschlüsselter Form durch Zugriff der Darstellungseinheit auf die lokale Servereinheit erfolgt.

2. Vorrichtung nach Anspruch 1, dadurch gekennzeichnet, dass die Datenverarbeitungsvorrichtung so ausgebildet ist, dass das Entschlüsseln und/oder der Zugriff sowie das Darstellen erfolgt, nachdem die zugeordneten Schlüssel- oder Rekonstruktionsdatei durch zumindest einmaligen Datenübertragungskontakt mit der externen Servereinheit (14) über das elektronische Datennetz (12) geladen und in der lokalen Servereinheit (24) zumindest teilweise abgelegt worden sind.

3. Vorrichtung nach Anspruch 1 oder 2, dadurch gekennzeichnet, dass die lokale Servereinheit (24) so ausgebildet ist, dass sie nicht über einen dienstspezifisch vordefinierten Standardport zugreifbar ist und bevorzugt eine Portadresse aufweist, die oberhalb von 1024 liegt.

4. Vorrichtung nach einem der Ansprüche 1 bis 3, dadurch gekennzeichnet, dass eine Adressierung der lokalen Servereinheit mit TCP/IP 127.0.0.1 oder local host erfolgt.

5. Vorrichtung nach einem der Ansprüche 1 bis 4, dadurch gekennzeichnet, dass die Darstellungseinheit (20) als lokale Viewereinheit, insbesondere Internet-Browser oder Office-Viewer, ausgebildet ist.

6. Vorrichtung nach einem der Ansprüche 1 bis 5, dadurch gekennzeichnet, dass die Darstellungseinheit (24) so ausgebildet ist, dass der Steuerbefehl zum Zugreifen auf das elektronische Dokument durch eine Funktionalität derselben, insbesondere ein dafür vorgesehenes Plug-in, generierbar ist.

7. Vorrichtung nach einem der Ansprüche 1 bis 6, dadurch gekennzeichnet, daß die Daten des elektronischen Dokuments aus einer Folge von Informationskomponenten einer Metasprache in Form einer Schriftsprache, eines Zahlensystems oder von Informationskomponenten aus in einer vorbestimmten, einheitlichen Formatstruktur angeordneten Datenelementen, insbesondere Bild-, Ton- oder Programminformationen, bestehen
und die verschlüsselten Daten durch ein Vertauschen und/oder Entfernen einer Informationskomponente in der Folge und/oder Hinzufügen einer Informationskomponente an eine vorbestimmte Position in der Folge von Informationskomponenten und/oder Austauschen einer Informationskomponente gegen eine bevorzugt in den Daten ursprünglich nicht enthaltene Informationskomponente
sowie durch Erzeugen der Schlüssel- oder Rekonstruktionsdatei mit Angaben über die vertauschten, entfernten, hinzugefügten und/oder ausgetauschten Informationskomponenten realisiert sind.

8. Vorrichtung nach einem der Ansprüche 1 bis 7, dadurch gekennzeichnet, dass die elektronischen Daten des elektronischen Dokuments durch einen mathematischen Algorithmus verschlüsselt in der lokalen Speichereinheit speicherbar sind.

9. Vorrichtung nach einem der Ansprüche 1 bis 8, dadurch gekennzeichnet, dass eine Verbindung (34) zwischen der Darstellungseinheit und der lokalen Speichereinheit so realisiert ist, dass elektronische Daten darüber in verschlüsselter Form ausgetauscht werden.

10. Vorrichtung nach Anspruch 9, dadurch gekennzeichnet, dass die ausgetauschten Daten lokal verschlüsselt und insbesondere nach dem Secure-Socket-Layer-Protokoll verschlüsselt sind.

11. Vorrichtung nach einem der Ansprüche 1 bis 10, gekennzeichnet durch der lokalen Servereinheit in der Datenverarbeitungsvorrichtung zugeordnete Identifikations- und/oder Authentifizierungsmittel (26) für einen Benutzerzugriff.

14-07-00

Fig.1